Thesis

10. Turvallisuusjohdon koulutusohjelma 10.1.2010

IT –system, -project or –process risk assessment
method and process

10. Turvallisuusjohdon
koulutusohjelma
Teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma15.2.2010
Pekka Ristimäki

INDEX

Definitions

ARS: Action Request System by BMC Software. Used as inventory and configuration database.

Risk: An expression of the likelihood that a defined threat will target and successfully exploit a specific vulnerability of an asset or business operation and cause a predicted set of consequences

Risk Identicication: The formal process of examining, analyzing and documenting the security of an organization's information technology**.**

Risk Assessment: A documented result of the risk identification process.

Risk Control: The process of applying controls to reduce the risk to an organization's data and information systems.

Risk Management: The process of identifying vulnerabilities in an organization's information system and taking steps to assure its confidentiality, integrity and availability.

NORA: Neste Oil Risk Assessment.A name for a method and process. The references used for creating NORA are Cause and Consequence Analysis (CCA), OCTAVE (CERT) and Information Security Forum's (ISF) IRAM –method.

RATE: Risk Assessment Team

RATE leader: IT Security, Corporate Security or other specialist, who is familiar with NORA. Leads the NORA Risk Assessment process.

Asset: The organizational resource that is being protected. An asset can be logical, such as a Web site, Help Desk, or information owned or controlled by the organization. An asset can be also physical, such as a server or a firewall cluster.

Threat: An object, person or other entity that represents a danger to an IT asset.

Threat assessment: The examination of a danger to assess its potential impact an organization.

Vulnerability is a weakness or a fault in a system or protection mechanism that exposes information to attack or damage.

Vulnerability Assessment (VA): The process of identifying and documenting specific and provable flaws in the organization's information asset environment.

Likelihood: The overall rating of the probability that a specific vulnerability within an organization will be successfully attacked. The formula: likelihood= threat * vulnerability

Business Impact Analysis (BIA): Crucial component of the initial risk assessment stages providing scenarios of the potential impact each attack or flaw could have on the organization.

ISF: Information Security Forum.

IRAM: ISF Risk Assessment Method

1 Background

Neste Oil has set IT risk management and information security principles to define, manage and minimize IT related risks for businesses. They also define functions, responsibilities, guidelines and processes for information security management. Neste Oil executive board has defined information as an important resource for business. Confidentiality, integrity and availability of information is important for business competitiveness. IT Risk Management and information security principles cover the usage of information, usage of IT technology, IT service processes and processes for managing IT risks and information security. Control of sub-contracted important IT services is in the scope to ensure partners' and suppliers' quality level of information security practices.

Information consists of documents, data bases, records, reports and spoken word. Technology consists of automation systems, operational systems (applications), office systems (PC’s, printers and PDAs) and infrastructure systems (servers, data communications and telecommunications).

2 Objectives

Objective of IT risk management is to ensure continuity, availability, integrity and confidentiality of critical business information and IT systems supporting the business. This will be done by identifying the risk, assessing its impact and making business decisions accordingly. In order to fulfill this objective and enable business competitiveness and continuity, a formal procedure for identifying and controlling the risks facing Neste Oil’s IT assets is needed.

IRAM tools have been used occasionally for assessing the risks related to Neste Oil’s most important IT –systems. However, also a more robust and simpler method is needed.

The objectives of this thesis are:

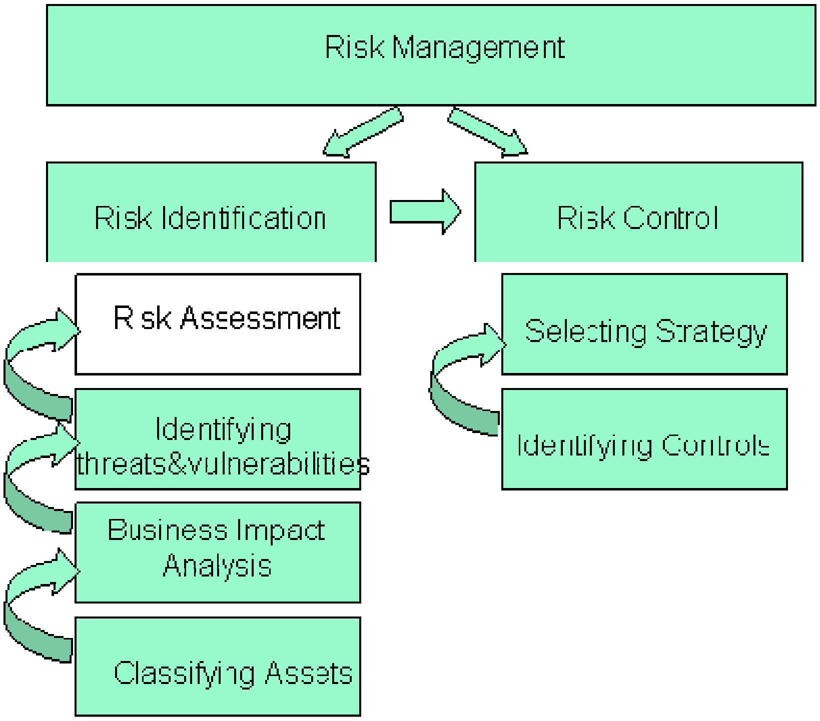
- Define a process and method, a concrete tool, for conducting risk assessments
- Method must suit for IT –asset, -process and –project risk assessment.

This document does not include instructions how to use NORA II (IRAM) supporting software tools (BIA Assistant, T&VA Assistant, CS Assistant). Each Risk Assessment Team (RATE) will be given instructions of the tools at introduction (T3) phase of the risk assessment process.

3 IT Risk Management overview

The formal process of identifying and controlling the risks facing organization is called risk management. Risk Management process consists of two parts: risk identification and risk control. Risk identification means examining and documenting the security of an organization's information technology. Risk control is the process of applying controls to reduce the risks to data and information systems. The various components of risk management are shown in figure 1.

Figure 1 Components of Risk Management



Once the assets have been identified and classified, a business impact analysis can be conducted. For example, what is the potential loss if this asset is unavailable for one hour, one day or one week? Assets are the targets of various threats, and the goal is to protect the assets from the threats. This is done by identifying the threats against the asset and also the vulnerabilities in asset environment or set up that could lead to unwanted incident. Risk Assessment assigns a rating for each identified risk. In relative risk assessment, risk rating equals likelihood of exploitation of a specific vulnerability *times* the business impact.

[Principles of Information Security]

The next phase is to identify controls that mitigate either the impact and/or likelihood of the risk. A control may be a technical security mechanism, policy or procedure. Finally one of the four strategies can be selected to manage the risk:

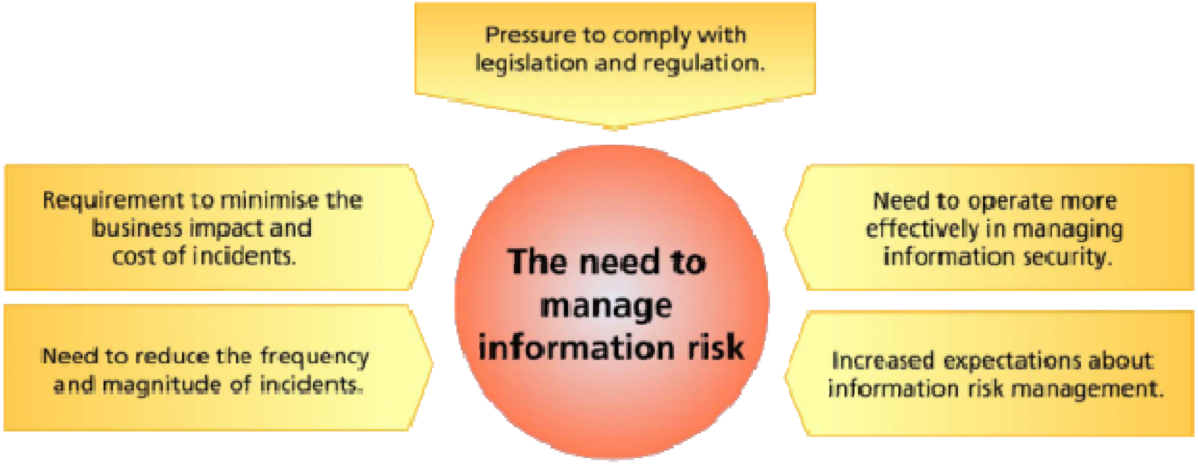
- Avoidance. The risk is unacceptable and the other strategies not effective.
- Transference. Transfer the risk to outside entities (insurance) or share the risk (partner or joint venture)
- Mitigation. Reduce the impact or likelihood of the risk.
- Acceptance. Understand the consequences and accept the risk without controls.

[Principles of Information Security]

3.1 Why do information risk analysis?

In addition to the damaging impact and cost of incidents there are a number of other drivers for organisations to manage information risk more effectively, including the pressure to comply with legal and regulatory requirements (such as PCI DSS) and the drive towards improved operational efficiency in information security. These requirements create pressure upon organisations to ensure they are managing information risk effectively.

Figure 2 Pressure for IT Risk Management


Pressure to comply with legislation and regulation.
Requirement to minimise the business impact and cost of incidents.
The need to manage information risk
Need to operate more effectively in managing information security.
Need to reduce the frequency and magnitude of incidents.
Increased expectations about information risk management.

[ISF IRAM methodologies project]

Information risk analysis is a practical approach to information risk management that drives down risk and minimises the likelihood of damaging incidents Information risk analysis must be relatively straightforward easy-to-use process. There are many benefits that can be gained by organisations undertaking information risk analysis. Many of these are associated with improving the overall effectiveness of information security and include items such as:

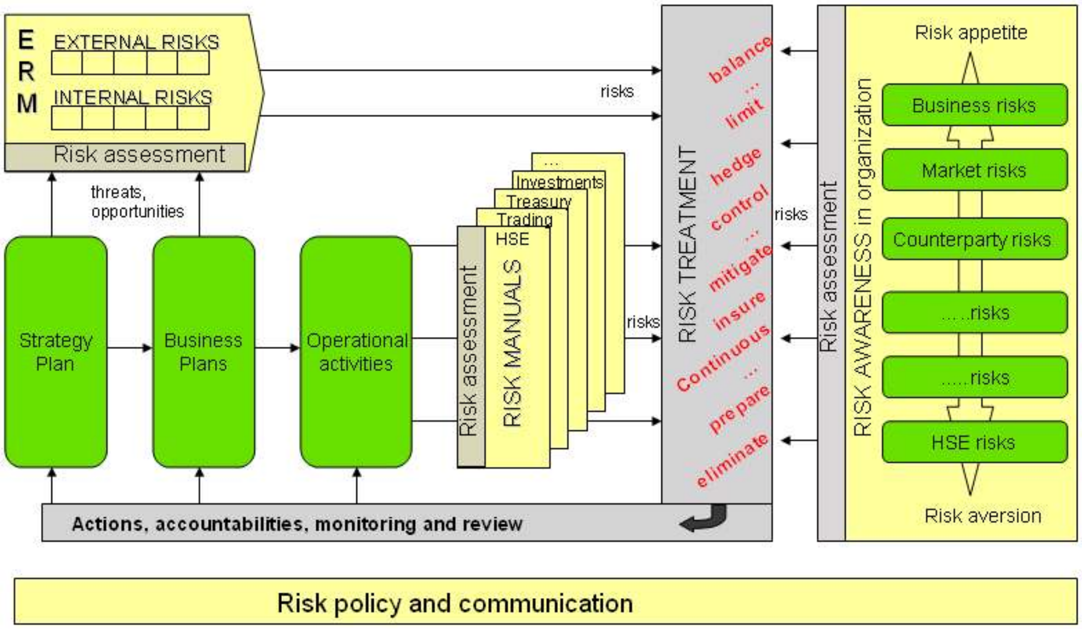
- Reducing the frequency and magnitude of incidents
- Meeting legal and regulatory requirements
- Rising awareness about information risk
- Increasing the level of trust from customers
- Focusing scarce resources where they will have the most effect

[ISF IRAM methodologies project]

4 Neste Oil Risk Management Framework

The framework describes the high level structure of risk management in Neste Oil.

Figure 3 Risk Management Framework



[Neste Oil Risk Management Principle (2010)]

Risk assessment

Risk assessment in Neste Oil is based on Enterprise Risk Management (ERM) process**,** risks manuals for specific disciplines and risk awareness in the organization. ERM process is a systematic way of identifying threats and opportunities in strategy targets and business plans. Risks are assessed, and means as well as accountabilities in risk treatment are set and included in our business processes.

Risk awareness

Through risk awareness all employees and teams are assessing risks in their daily work when making business and operational decisions and actions. Risk manuals consist of risk principles, guidelines and instructions. In the manuals risk disciplines are described and operational responsibilities, mandates and limits are set. Manuals can also include detailed guidance on risk identification techniques. In these specific risk disciplines, risks are continuously assessed and treated. Risk awareness in the organization is based on behaviour of individual employee. The level of risk awareness is dependent of adoption of right risk attitude and knowledge. Risk awareness is constantly improved by communicating company values, targets and policies, as well as by training personnel in risk management. The risk treatment methods are used according to communicated risk appetite or risk aversion.

Risk treatment

Risk treatment methods in Neste Oil are dependent on risk appetite or risk aversion within the risk discipline in question. For instance in sales decisions are generally based on the balance between risk and reward. On the other hand in safety issues there is a strong aversion to risks and Neste Oil does not make compromises in risk treatment on financial basis.

Risk monitoring

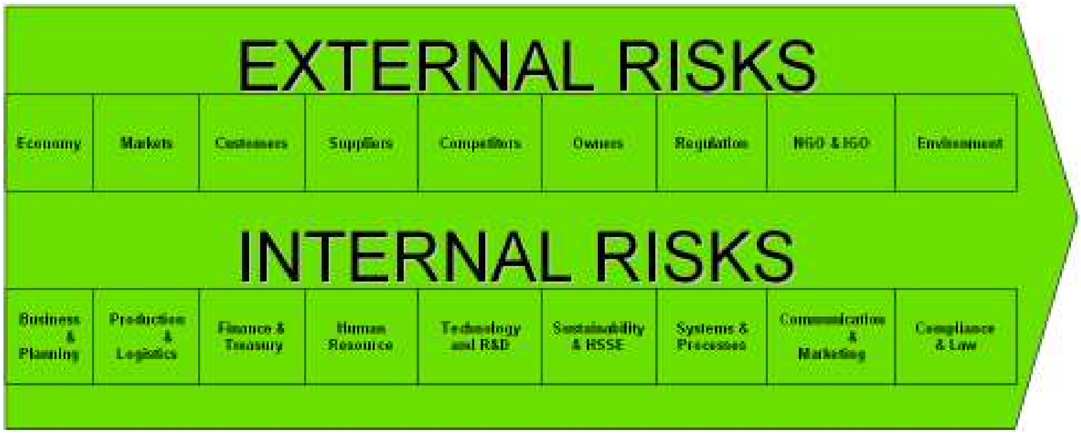
Effectiveness of the risk management is monitored, reviewed and constantly improved through audits and performance reviews.

[Neste Oil Risk Management Principle (2010)]

Risk categories and disciplines

For risk categories there is an external and internal perspective.In internal risk category used disciplines are the functions, which are mainly according to responsibilities in the organization. Those are finance & treasury, human resource, technology and R&D, sustainability and HSSE, systems and processes etc. In external risk category used disciplines are economy, markets, counterparty (customers, suppliers), competitors, owners, regulations, NGO & IGO's and environment.

Figure 4 Risk Categories



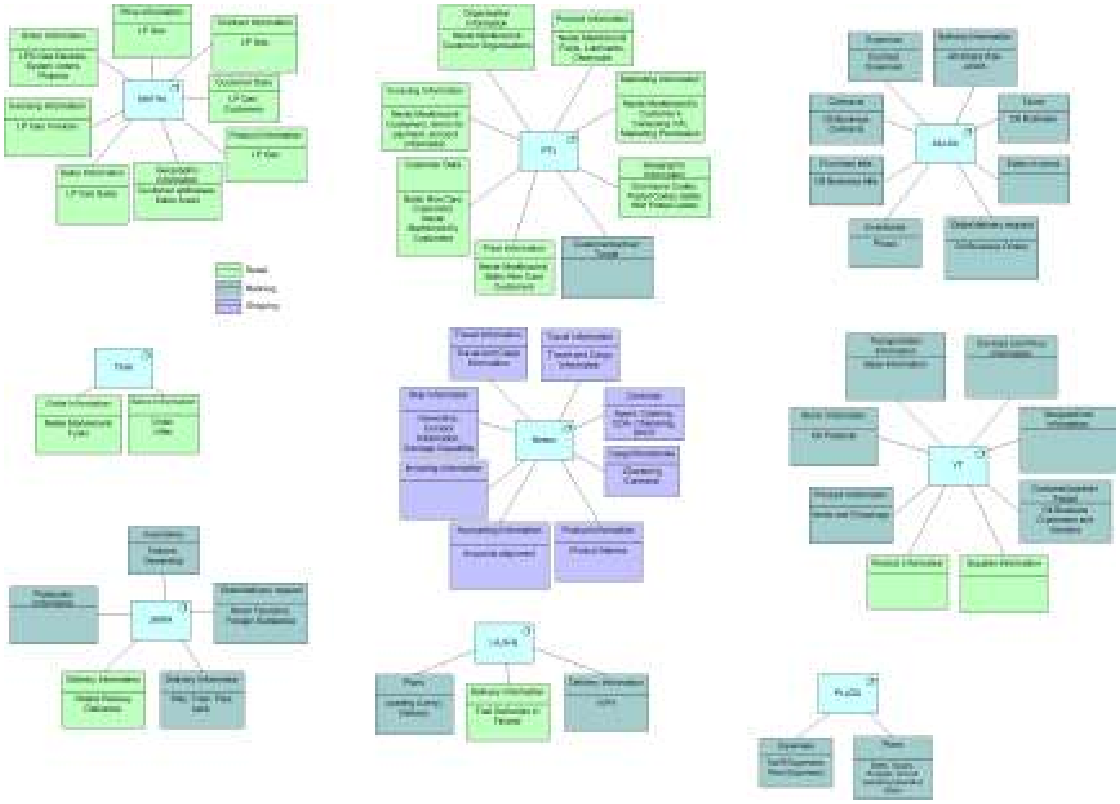
[Neste Oil Risk Management Principle (2010)]

5 Asset Classification

One important input for asset classification in Neste Oil is a careful study of processes, data/information content and data/information flows between the processes. Sources of master data and their business owners have been identified. The result is architectural description of the main processes, main information elements, data flows and current applications and interdependencies. Assets are being classified based on their importance in business processes. Figure 5 illustrates the master data sources in Neste Oil. The figure is in Appendix 1 (full size).

[Neste Oil Information Architecture Study, TietoEnator 2007]

Figure 5 Neste Oil master data sources



Assets class correlates directly to the business impact in case that particular asset is not available, or the integrity or confidentiality of the asset is compromised. The relative importance of the asset is based on its impact on revenue, profitability or public image. Neste Oil uses Remedy ARS for managing the IT assets. The class of an asset is stored to ARS inventory registry.

[Neste Oil Information Architecture Study, TietoEnator 2007]

The asset classes and descriptions are listed in table 1.

Table 1 Asset classes

Class	**Description**
Low	Total malfunction or loss of the asset causes low or no impact to corporate business critical function. No image loss, low financial loss.
Medium	Total malfunction or loss of the asset causes moderate impact to corporate business critical function for an extended period. Moderate image and/or financial loss.
High	Total malfunction or loss of the asset causes high loss of corporate business critical function for an extended period. Severe image and/or financial loss.

6 Analyzing Risk Severity

6.1 General

When the risks and the root causes have been identified, risks will be analyzed. The aim is to estimate the impact to the business and likelihood of the risk to occur. Risk likelihood can be reversely compared to the possible impact of the event. The following table illustrates the relationship.

Table 2 Risk predictability

Risk Severity	**Likelihood (frequency)**	**Impact (expected loss)**	**Predictability**
Low	High	Low	Event will likely happen in <1 year period
Medium	Medium	Medium	Event will likely happen in 1<5 years period
High	Low	High	Not easy to predict

In general, based on the table, low impact events happen often and their predictability is fairly easy. On the other hand, the frequency of high impact events is low but the impact is high and their predictability is not easy.

6.2 Likelihood and Impact rating

The following tables give guidance for rating the likelihood and impact.

Table 3 Risk likelihood rating.

Frequency	Likelihood rating	Likelihood description
1/100 (once in 100 years)	1	Very unlikely Event such as total destruction of data center
1/10 (once in ten years)	2	Unlikely Event such as major electricity break out in large area
1/1 (once a year)	3	Possible Event such as DoS attack against Neste Oil service(s)
10/1 (monthly)	4	Very possible Event such as employees user ID not deactivated after resignation
100/1 (weekly)	5	Weekly Event such as a malware/spyware in one or several workstations

Table 4 Risk impact rating

Impact on Reputation*	Impact on Business*	Impact rating	Impact description
Insignificant	<1000€	1	Insignificant
Very limited media coverage or site neighbourhood concern	1000€<10000€	2	Minor
Limited media coverage Some impact on local level activities	10000€ <100000€	3	Medium
Potential brand impact. Persistent national concern.	100000€<1 0000000€	4	Significant
Substantial adverse media attention. International concern. Persistent, intense, national, public, political and media scrutiny. Severe negative reputational impact	>1000000€	5	Intolerable

- *Rating can be based on reputation or monetary loss*

[Yrityksen riskienhallinta]

Analyzing the likelihood and the impact is not enough. When estimating the severity of the risk, the impact has to be emphasized. The impact of the event has direct influence on the business continuity. On the worst scenario the result is bankruptcy. When emphasizing the impact, the focus of the mitigating actions can be directed to the most severe scenarios.

The formula for calculating the risk rating: ***Risk likelihood * Impact² = Risk rating***

Table 5 Risk rating and mitigating actions

Risk rating	**Significance**	**Mitigation actions**
<26	Insignificant	Poses no threat to the company. No mitigation actions required.
26-63	Moderate	Mitigation action required. Cost and benefits of mitigation actions must be carefully analyzed.
>63	Significant	*Mitigation actions have to be started immediately.* *Further actions, or a start, (project, system implementation etc) must be halted until the risk has been mitigated or eliminated.*

[Yrityksen riskienhallinta]

7 Risk Assessment Process

Task	**Description**	**Responsible +members**	**Tool**
T1	Initiate Risk Assessment process by contacting IT Security. Send the preliminary information of the system(s) and/or project (PIP)	Project Manager System Manager	Email NORA System Information Form (Appendix 4) Project Information Paper (PIP)
T2	**Workshop 1:** Risk Assessment preparation Nominate RATE members Set up the schedule and decide the number of ws's.	RATE leader+ Project Manager and/or System manager	NORA Preparation Form (Appendix 6)
T3	**Workshop 2:** ➢ NORA introduction Business Impact Analysis ➢ Threat and Vulnerability Assessment Assessment	RATE leader+ RATE members	**NORA I:** NORA Assessment Form (Appendix 7) **NORA II:** BIA Assistant T&VA Assistant
T4	**Workshop 3:** Mitigation / Control selection	RATE leader+ IT Specialists	**NORA I:** NORA Assessment Form (Appendix 7) NORA Risk Register Form (Appendix 8) **NORA II**: CS Tool
T5	Follow Up meeting Status of the implementation of the mitigating actions	RATE leader+ Project Manager and/or System manager	NORA Follow Up Form (Appendix 9)

NOTE: Tasks T3-T4 can be conducted in one workshop if only NORA I method is used.

8 Neste Oil Risk Assessment Method (NORA)

NORA is a combination of two methods which can be used either together or individually. NORA I is a simple risk assessment method which can be used when determining risks related to specific IT-project, -process or –asset that is classified *Medium* of *Low*. This method is based on Fault Tree analysis which is part of the Cause Consequence Analysis (CCA) .NORA II, which is based on ISF's IRAM, is recommended to be used when:

- The target of an assessment is an IT-asset classified as *High.*
- The target of an assessment is a project or process that includes IT-asset(s) classified as *High.* In this case, both NORA I and II will be used.

Risk Assessment has to be conducted once a year for every IT –process or –asset that is classified High or Medium.

8.1 NORA I

The basis for NORA I method is fault tree analysis (FTA) which is part of the Cause and Consequence Analysis (CCA). Cause-consequence analysis (CCA) is a blend of fault tree and event tree analysis. This technique combines cause analysis (described by fault trees) and consequence analysis (described by event trees), and hence deductive and inductive analysis is used. The purpose of CCA is to identify *the root cause* for the chains of events that can result in undesirable consequences. With the probabilities of the various events in the CCA diagram, the probabilities of the various consequences can be calculated, thus establishing the risk level of the system. Finding the root cause makes it easier to focus the mitigating actions correctly and cost effectively. This technique was invented by RISO Laboratories in Denmark to be used in risk analysis of nuclear power stations. NORA I risk assessment can be conducted in one or two workshops.

8.1.1 Risk assessment workshop(s) (T3-T4)

The number of workshops carried out will be determined on the basis of the nature, size and complexity of the asset, business process or project and the risk environment. This will be determined by the Risk Assessment Team (RATE) leader together with the project manager and/or system manager (task 2 in the process). Essentially it is a qualitative process, involving the following steps ((tasks T3-T4 in the process):

NORA I

1. Establish the context of the risk assessment. Whether assessing an asset, project or business operation:
   - real and measurable objectives need to be defined; and
   - the key (or critical) assets or operations – people, property, information, production or sales operations, suppliers, transport and communications systems – need to be identified.
2. Identify possible threats to the asset, project or business process. Each RATE member identifies threats individually. (It may help to categorise threats into such areas as: security, political, environmental, operational).
3. NORA Assessment Form (Appendix 7) will be used as a working tool in steps 4-7.
4. The threats are pooled and each RATE member is allocated a certain number of votes, which will be defined within team, to rank the threats in terms of their potential harmfulness to Neste Oil. Stickers will be used at this phase. In assessing the potential harm, the RATE members should consider *the likelihood* of the event occurring and the severity or *impact* of the event on the business. Likelihood and impact classes are described in the Appendix 2: Likelihood and Impact classes.
5. Brainstorming is used and events are prioritized in terms of their potential risk to Neste Oil and on the basis of the number of votes allocated to each event by the RATE members. Risk prioritisation classes are described in the Appendix 3: Risk classes
6. For each High rated risk a Fault Tree is created to determine the underlying cause
7. For each underlying cause, a preventative or corrective action should be identified.
8. Results should be recorded in the Appendix 8: Risk Register and Treatment Plan
9. When the expected loss exceeds one million euros, the risk must be ported to the ERM.

NORA II

- The assistant tools will be introduced at the beginning of each workshop.
- The tools guide through the assessment process.

8.1.2 Fault Tree Analysis (FTA)

Fault Tree is a tool for workshop members and can be used for identifying the root causes for unwanted events. Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential unwanted event called a TOP event, and then determining all the ways it can happen. The analysis proceeds by determining how the TOP event can be caused by individual or combined lower level failures or events. The individual causes for unwanted event are identified at the bottom of the tree and effective controls can be assigned at this level. The causes of the TOP event are connected through logic gates. Only AND-gates and OR-gates are used in NORA I.
[SANS 17799/27001 Security and Audit Framework, 2008]

8.1.2.1 Fault Tree construction

Fault Tree construction includes the following steps:

1. Define the TOP event in a clear way.

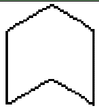
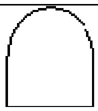
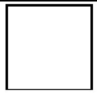
   Should always answer:
   What e.g., “emails from oil tanker unsuccessfull”
   Where e.g., “port of Rotterdam”
   When e.g., “During normal working hours ”
2. Determine what are the immediate, necessary, and sufficient events and conditions causing the TOP event.
3. Connect via AND- or OR-gate (The logic gates used should be restricted to the and gate and or gate.)
4. Throughout this process, a tree diagram is used to record the events as they are identified. Tree branches stop when all events leading to the negative event are complete.
5. Validate the tree for completeness and accuracy.

[System Reliability Theory (2nd ed), Rausand&Hoyland, 2004]

8.1.2.2 Fault Tree symbols (gates)

Symbols are used to represent various events and describe relationships.

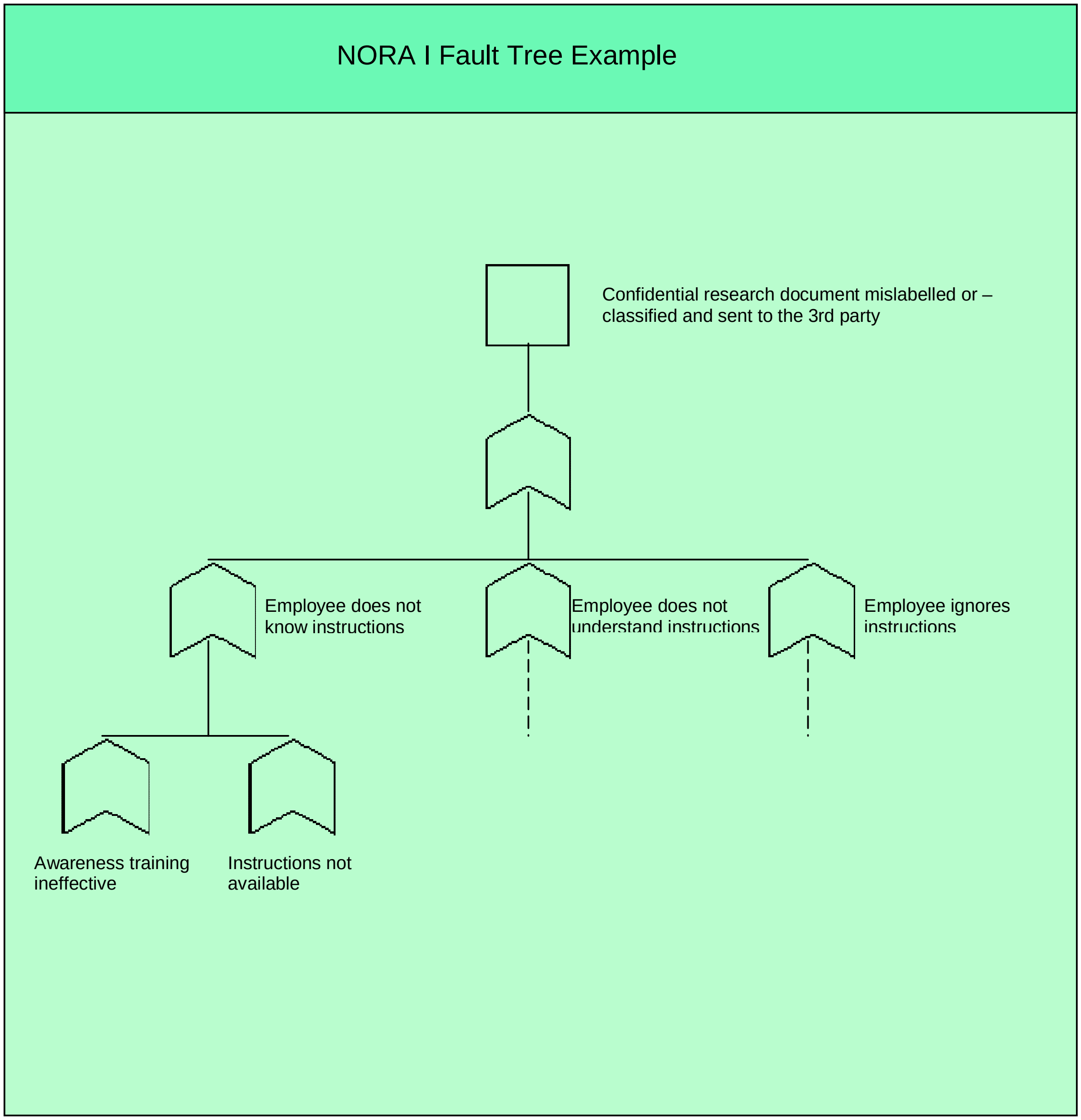
Table 2 Fault Tree symbols

Symbol	Description
	Or gate – represents a situation in which any of the events shown below the gate (input gate) will lead to the event shown above the gate (output event). The event will occur if only one or any combination of the input events exists.
	And gate – represents a condition in which all the events shown below the gate (input gate) must be present for the event shown above the gate (output event) to occur. This means the output event will occur only if all of the input events exist simultaneously.
	Rectangle – represents the negative event and is located at the top of the tree. This is the only symbol that will have a logic gate and input events below it.

[System Reliability Theory (2nd ed), Rausand&Hoyland, 2004]

8.1.2.3 Fault Tree example

Figure 6 Fault Tree example


NORA I Fault Tree Example
Confidential research document mislabelled or – classified and sent to the 3rd party
Employee does not know instructions
Employee does not understand instructions
Employee ignores instructions
Awareness training ineffective
Instructions not available

8.2 NORA II

NORA II uses ISF's information risk analysis methodology (IRAM) and supporting software tools (BIA Assistant, T&VA Assistant, CS Assistant). IRAM helps to determine the information risks in IT system and determine the controls required to mitigate those risks. There are three phases in the IRAM methodology: Phase 1 – Business Impact Assessment, Phase 2 – Threat and Vulnerability Assessment, Phase 3 – Control Selection. Each phase is dependent on the completion of the previous phase and all phases must be completed to undertake an information risk analysis.

This document does not provide detailed information on how to undertake information risk analysis using IRAM process and tools. This is merely an introduction to the method. The process and supporting tools are fully documented and the Rate team leaders will be properly trained.

[ISF IRAM methodologies project]

Table 3 IRAM methodology phases

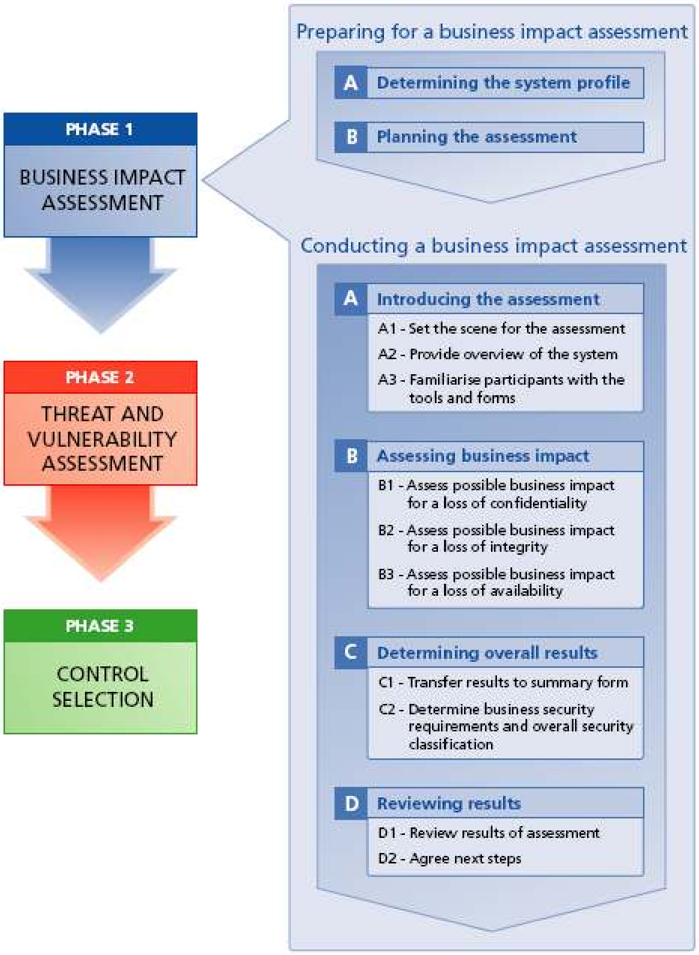
Phase	Tool	Purpose of the phase	Main output
1. Business Impact Assessment (BIA)	BIA assistant	To assess possible business impact and determine the business security requirements for protecting information in the system.	• Business Impact Rating forms • Business Impact Assessment summary form
2. Threat and Vulnerability Assessment (T&VA)	T&VA assistant	To determine the threats and vulnerabilities that increase the likelihood of incidents occurring in a system.	• Threat assessment report • Vulnerability assessment report • Detailed Security requirements report
3. Control Selection (CS)	CS assistant	To evaluate and select controls to reduce the likelihood of incidents occurring.	• Control evaluation report • Control selection report

[ISF IRAM methodologies project]

8.2.1 Business impact analysis (BIA)

A business impact assessment is a method of determining the possible business impact that an organisation could experience as a result of an incident that compromises information (eg in a system such as a key business application). Conducting a business impact assessment (BIA) enables organisations to gain a clear viewof the importance of information stored in or processed by a system and the requirement to protect its confidentiality, integrity and availability. Business impact assessment helps identify the high-level security requirements and appropriate next steps that need to be taken to protect information. These parts and their key steps are shown in figure 7.

Figure 7 BIA main parts and steps


PHASE 1
BUSINESS IMPACT ASSESSMENT
PHASE 2
THREAT AND VULNERABILITY ASSESSMENT
PHASE 3
CONTROL SELECTION
Preparing for a business impact assessment
A Determining the system profile
B Planning the assessment
Conducting a business impact assessment
A Introducing the assessment
A1 - Set the scene for the assessment
A2 - Provide overview of the system
A3 - Familiarise participants with the tools and forms
B Assessing business impact
B1 - Assess possible business impact for a loss of confidentiality
B2 - Assess possible business impact for a loss of integrity
B3 - Assess possible business impact for a loss of availability
C Determining overall results
C1 - Transfer results to summary form
C2 - Determine business security requirements and overall security classification
D Reviewing results
D1 - Review results of assessment
D2 - Agree next steps

[ISF IRAM methodologies project]

The key characteristics of a business impact assessment are that it should be:

- business-oriented (eg involves key business staff in the assessment of business impact)
- non-technical (eg uses business language)
- easy to undertake (eg uses simple tools and a clear approach)
- relatively quick (eg takes less than 3 hours to undertake)
- self-contained (eg produces immediate results and feedback to participants).

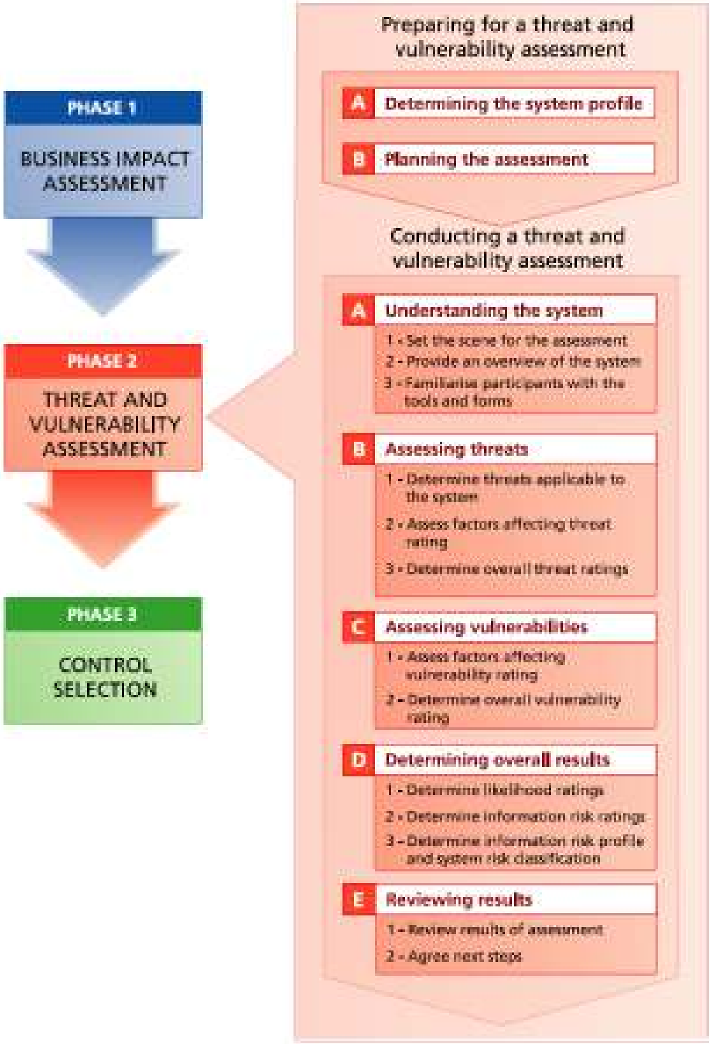
8.2.1.1 Business Impact Reference Table (BIRT)

The IRAM approach to business impact assessment is based on organisations using their own pre-defined, organisation-specific, Business Impact Reference Table (BIRT). BIRT enables non-specialists to make well-informed judgements about the level of business impact that could occur in the event of an incident that compromises the confidentiality, integrity or availability of information.
[ISF IRAM methodologies project]
An example of BIRT is in Annex 10.

8.2.2 Threats and vulnerabilities (T&VA)

Threat and vulnerability assessment is a method to assess the range of threats that could compromise information (eg in a system such as a key business application) and the vulnerabilities in that system that could lead to information being compromised. Assessing the range of threats and vulnerabilities to information provides the organisation with an understanding of the likelihood of incidents occurring.

Threat and vulnerability assessment makes use of the high-level business security requirements that are derived from the business impact assessment process and helps identify the detailed security requirements for a system (ie the key information risks that should be mitigated) (see figure 8).
[ISF IRAM methodologies project]
Figure 8 T&VA main parts and steps


PHASE 1
BUSINESS IMPACT ASSESSMENT
PHASE 2
THREAT AND VULNERABILITY ASSESSMENT
PHASE 3
CONTROL SELECTION
Preparing for a threat and vulnerability assessment
A Determining the system profile
B Planning the assessment
Conducting a threat and vulnerability assessment
A Understanding the system
1 - Set the scene for the assessment
2 - Provide an overview of the system
3 - Familiarise participants with the tools and forms
B Assessing threats
1 - Determine threats applicable to the system
2 - Assess factors affecting threat rating
3 - Determine overall threat ratings
C Assessing vulnerabilities
1 - Assess factors affecting vulnerability rating
2 - Determine overall vulnerability rating
D Determining overall results
1 - Determine likelihood ratings
2 - Determine information risk ratings
3 - Determine information risk profile and system risk classification
E Reviewing results
1 - Review results of assessment
2 - Agree next steps

The key characteristics of a threat and vulnerability assessment are that it should be:

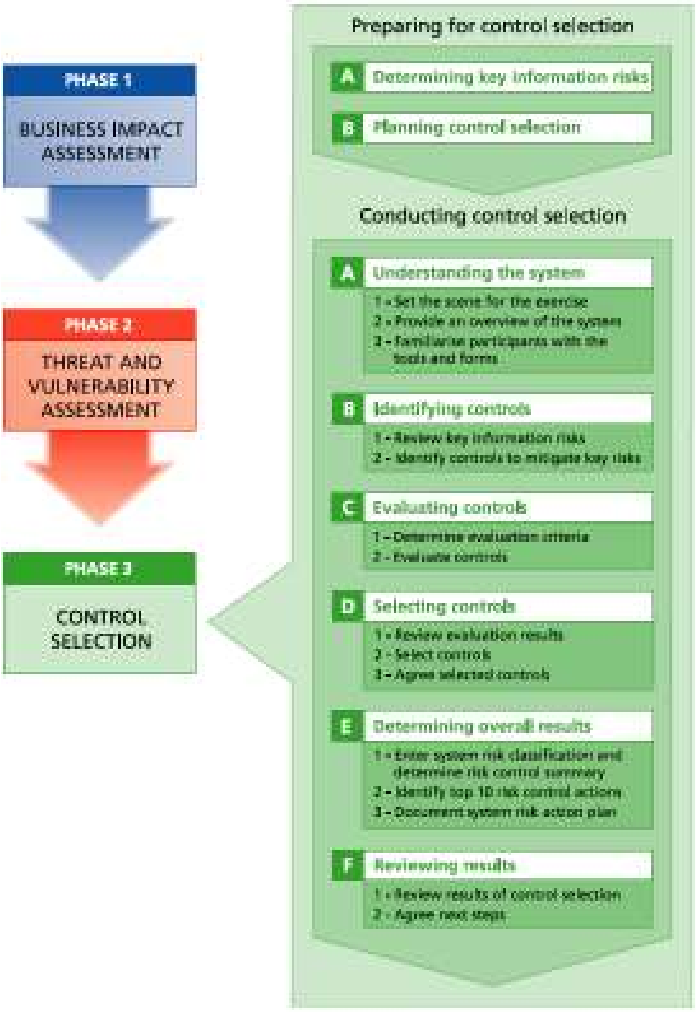
- technically-oriented (eg examines the technology solution in detail)
- undertaken by a skilled information risk analyst (eg requires a solid grounding in how threats and vulnerabilities can affect information)
- knowledge-dependent (eg requires good information on threats and vulnerabilities)
- easy-to-understand (eg produces clear results that can be acted on in the final phase of the information risk analysis process).

[ISF IRAM methodologies project]

An example of T&VA summary is in Annex 11.

8.2.3 Control selection (CS)

Control selection is a method to evaluate and select controls to mitigate information risk in a system. Control selection makes use of the detailed security requirements determined in the threat and vulnerability phase. It helps identify controls that meet the business requirements for security in the system being assessed, (see Figure 8).


PHASE 1
BUSINESS IMPACT ASSESSMENT
PHASE 2
THREAT AND VULNERABILITY ASSESSMENT
PHASE 3
CONTROL SELECTION
Preparing for control selection
A Determining key information risks
B Planning control selection
Conducting control selection
A Understanding the system
1 - Set the scene for the exercise
2 - Provide an overview of the system
3 - Familiarise participants with the tools and forms
B Identifying controls
1 - Review key information risks
2 - Identify controls to mitigate key risks
C Evaluating controls
1 - Determine evaluation criteria
2 - Evaluate controls
D Selecting controls
1 - Review evaluation results
2 - Select controls
3 - Agree selected controls
E Determining overall results
1 - Enter system risk classification and determine risk control summary
2 - Identify top 10 risk control actions
3 - Document system risk action plan
F Reviewing results
1 - Review results of control selection
2 - Agree next steps

[ISF IRAM methodologies project]

An example of Control Selection is in Annex 12.

9 Suggestions

- Business Information Reference Table (BIRT) should be created for each Business Area and Common Function (=> total four BIRT's)
- Risk Assessment should be integrated to System Development Framework –process (new systems)
- A project should be established to assess all class *High* IT assets
- Risk Assessment reports should be stored to centralized repository (NCR on Sharepoint)

10 References

1. Principles of Information Security, Michael E. Whitman and Herbert J. Mattord, 2005

2. System Reliability Theory (2nd ed), Rausand&Hoyland, 2004

3. SANS 17799/27001 Security and Audit Framework, 2008.

4. ISF IRAM methodologies project

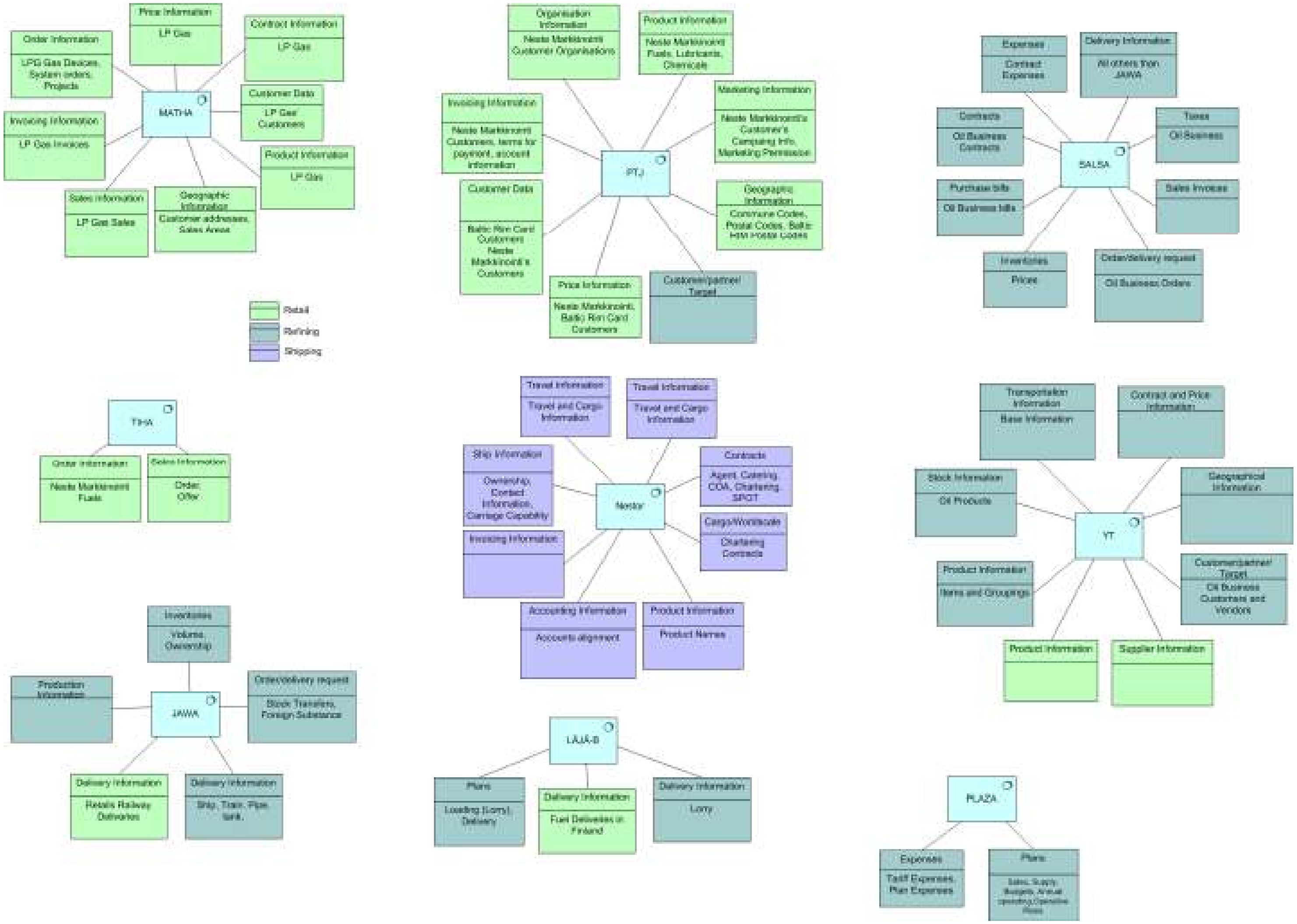
5. Neste Oil Information Architecture Study, TietoEnator 2007

6. Yrityksen riskienhallinta, Juvonen, Korhonen, Ojala, Salonen, Vuori. FINVA, 2008

7. Neste Oil Risk Management Principle (2010)

11 Appendices

11.1 Appendix 1 Neste Oil master data sources



11.2 Appendix 2 Likelihood and Impact classes

Risk likelihood rating

Frequency	Likelihood rating	Likelihood description
1/100 (once in 100 years)	1	Very unlikely
1/10 (once in ten years)	2	Unlikely
1/1 (once a year)	3	Possible
10/1 (monthly)	4	Very possible
100/1 (weekly)	5	Weekly

Table 4 Risk impact rating

Impact on Reputation*	Impact on Business*	Impact rating	Impact description
Insignificant	<1000€	1	Insignificant
Very limited media coverage or site neighbourhood concern	1000€<10000€	2	Minor
Limited media coverage Some impact on local level activities	10000€ <100000€	3	Medium
Potential brand impact. Persistent national concern.	100000€<1 0000000€	4	Significant
Substantial adverse media attention. International concern. Persistent, intense, national, public, political and media scrutiny. Severe negative reputational impact	>1000000€	5	Intolerable

** Rating can be based on reputation or monetary loss*

11.3 Appendix 3: Risk classes

Table 5 Risk rating and mitigating actions

Risk rating	**Significance**	**Mitigation actions**
<26	Insignificant	Poses no threat to the company. No mitigation actions required.
26-63	Moderate	Mitigation action required. Cost and benefits of mitigation actions must be carefully analyzed.
>63	Significant	*Mitigation actions have to be started immediately.* *Further actions, or a start, (project, system implementation etc) must be halted until the risk has been mitigated or eliminated.*

11.4 Appendix 4: NORA System Information Form

System Information		
General		
Service/System Name:		
Service/System Owner:		
Business Area/Function:	□ Retail □ Oil Products □ Refining □ P&L □ ICT □ Other Other:	
Service/System Role :	□ Production □ Test □ Development	
System Age:		
Key Contacts:		
Main Business Function: (eg Sales, Accounting, HR system, ICT infra, ERP)		
Description of the System/Service:		
Business Contribution		
Importance to the business:	□ Low □ Medium □ High	
Contributes to key business objectives:	□ Financial targets □ Operational efficiency □ Customer satisfaction □ Employee satisfaction	
Technical Information		
Network type:	□ Internet □ Intranet □ Extranet □ Other	
Number of platforms:	Servers:	Workstations:
Number of business users:	Internal:	External
Number of support users:	Internal	External
Additional Information		

11.5 Appendix 5: NORA Preparation Form

Task	Description	Participants	Date
T2	Workshop 1: Risk Assessment preparation Nominate RATE members Set up the schedule and decide the number of ws's.	RATE Leader: Rate members:	
T3	Workshop 2: ➢ NORA introduction Business Impact Analysis ➢ Threat and Vulnerability Assessment Assessment	RATE Leader: Rate members:	
T4	Workshop 3: Mitigation / Control selection	RATE Leader: Rate members:	
T5	Workshop 5: Follow up	RATE Leader: Rate members:	

11.6 Appendix 6: NORA Assessment Form

Date:	
Project/Process:	
Project/Process Business Division:	
RATE Team Leader:	
Project Manager(s):	
Business Representative:	
IT Representative:	
Other RATE members:	

Unwanted event	Likelihood 1-5	Impact 1-5	Risk Rating (Likelihood * Impact^2)	Corrective or preventive action(s)	Expected Loss (€)	Effect of corrective or preventive action Low/Medium/High

When assessment ready, transfer the results to the Risk Register Form

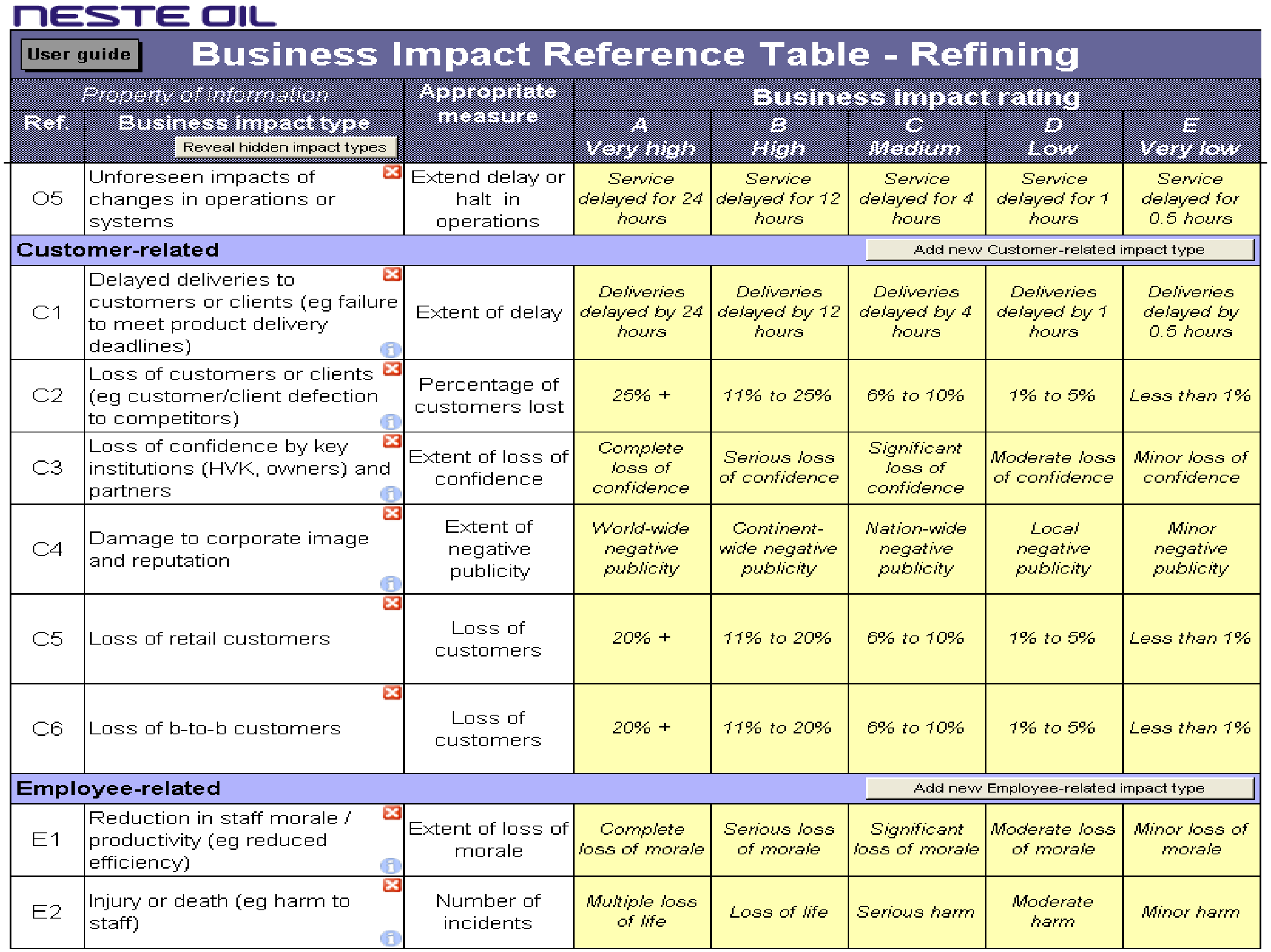
11.7 Appendix 7: NORA Risk Register

Rank in order of priority in the Risk Register the risks identified in the assessment by RATE. Determine risk treatment measures or controls and list them also in the Risk Register. Determine whether the risk treatment measures reduce the likelihood or the impact of the risk (or both) and determine the residual risk: that is, the remaining risk that needs to be managed. The residual risk is recorded in the Risk Register and Treatment Plan in the column *Post treatment risk category*

Risk	Treatment Objectives	Treatment Strategy	Date	Dependencies	Risk Owner	Post-treatment Risk Category	Cost *(€)*
In order of priority with colour rating	*Reduction in likelihood and/or impact*	*List of identified risk control measures – both improvements to existing controls and new control measures - with preferred options highlighted*	*Target date for implem-entting risk controls*	*Impact of risk treatment on investment/business or other risk treatments*	*Position responsible*	*Assessed level of risk after implementing risk mitigation. (Defined by colour rating**)***	*Cost of the control measure(s)*
Confidential research document sent to unauthorized recipient	**Likelihood**	**Awareness training** **Classification instructions** **Access controls** **Document management system**		**Resource costs (training days)**	**Project Manager**	🟨	
Confidential research document sent to unauthorized recipient	**Impact**	**NDA's**			**Project Manager**	🟥	

(There is a hypothetical risk to indicate the way in which the register should be complete)

11.8 Appendix 8: NORA BIRT



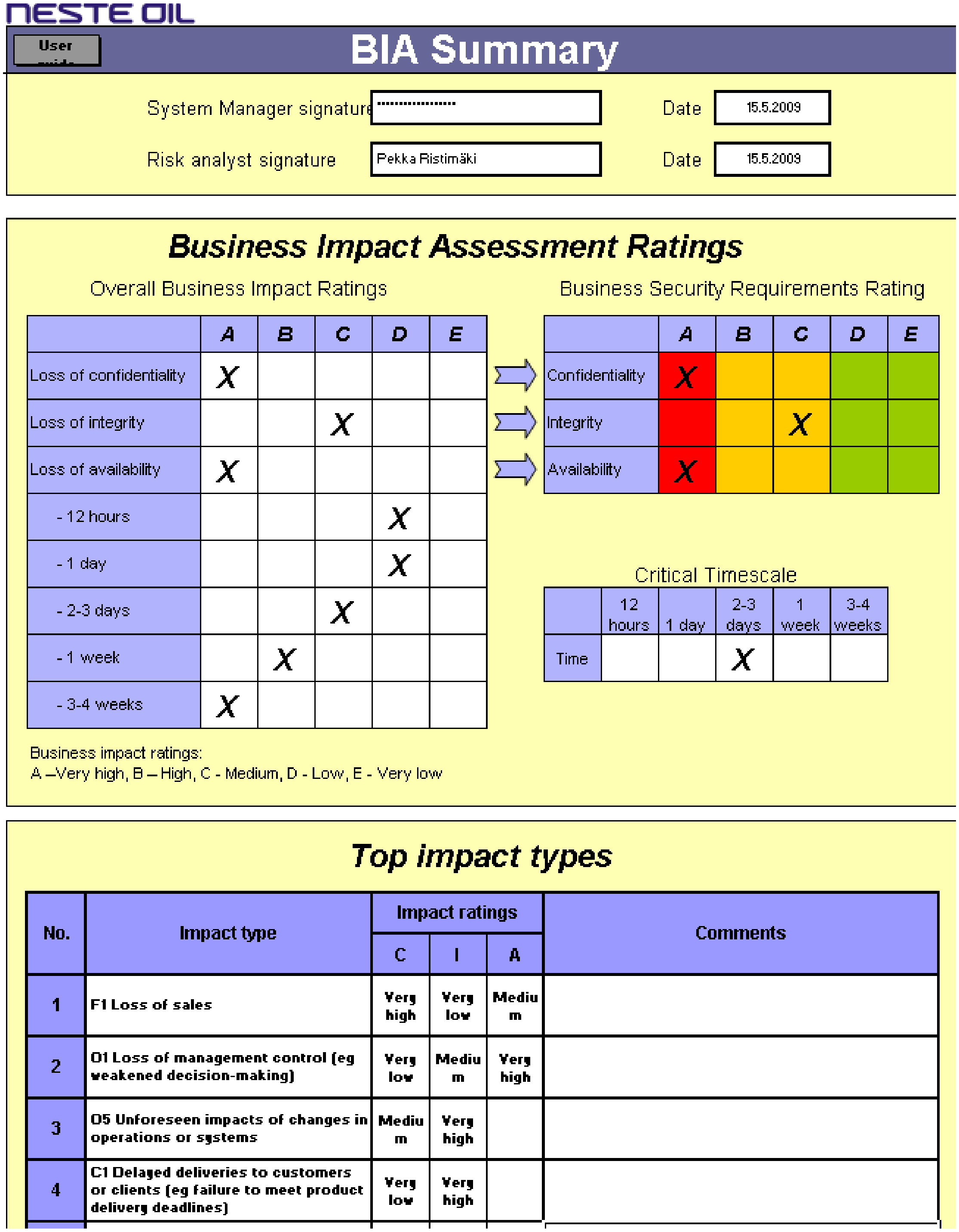
NESTE OIL

User guide

Business Impact Reference Table - Refining

Property of information		Appropriate measure	Business impact rating				
Ref.	Business impact type Reveal hidden impact types		A Very high	B High	C Medium	D Low	E Very low
O5	Unforeseen impacts of changes in operations or systems	Extend delay or halt in operations	Service delayed for 24 hours	Service delayed for 12 hours	Service delayed for 4 hours	Service delayed for 1 hours	Service delayed for 0.5 hours
Customer-related					Add new Customer-related impact type		
C1	Delayed deliveries to customers or clients (eg failure to meet product delivery deadlines)	Extent of delay	Deliveries delayed by 24 hours	Deliveries delayed by 12 hours	Deliveries delayed by 4 hours	Deliveries delayed by 1 hours	Deliveries delayed by 0.5 hours
C2	Loss of customers or clients (eg customer/client defection to competitors)	Percentage of customers lost	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%
C3	Loss of confidence by key institutions (HVK, owners) and partners	Extent of loss of confidence	Complete loss of confidence	Serious loss of confidence	Significant loss of confidence	Moderate loss of confidence	Minor loss of confidence
C4	Damage to corporate image and reputation	Extent of negative publicity	World-wide negative publicity	Continent-wide negative publicity	Nation-wide negative publicity	Local negative publicity	Minor negative publicity
C5	Loss of retail customers	Loss of customers	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%
C6	Loss of b-to-b customers	Loss of customers	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%
Employee-related					Add new Employee-related impact type		
E1	Reduction in staff morale / productivity (eg reduced efficiency)	Extent of loss of morale	Complete loss of morale	Serious loss of morale	Significant loss of morale	Moderate loss of morale	Minor loss of morale
E2	Injury or death (eg harm to staff)	Number of incidents	Multiple loss of life	Loss of life	Serious harm	Moderate harm	Minor harm

11.9 Appendix 9: NORA BIA Summary



NESTE OIL

User

BIA Summary

System Manager signature ………………… Date 15.5.2009

Risk analyst signature Pekka Ristimäki Date 15.5.2009

Business Impact Assessment Ratings

Overall Business Impact Ratings

	A	B	C	D	E
Loss of confidentiality	X				
Loss of integrity			X		
Loss of availability	X				
- 12 hours				X	
- 1 day				X	
- 2-3 days			X		
- 1 week		X			
- 3-4 weeks	X				

Business Security Requirements Rating

	A	B	C	D	E
Confidentiality	🟥 X	🟨	🟨	🟩	🟩
Integrity	🟥	🟨	🟨 X	🟩	🟩
Availability	🟥 X	🟨	🟨	🟩	🟩

Critical Timescale

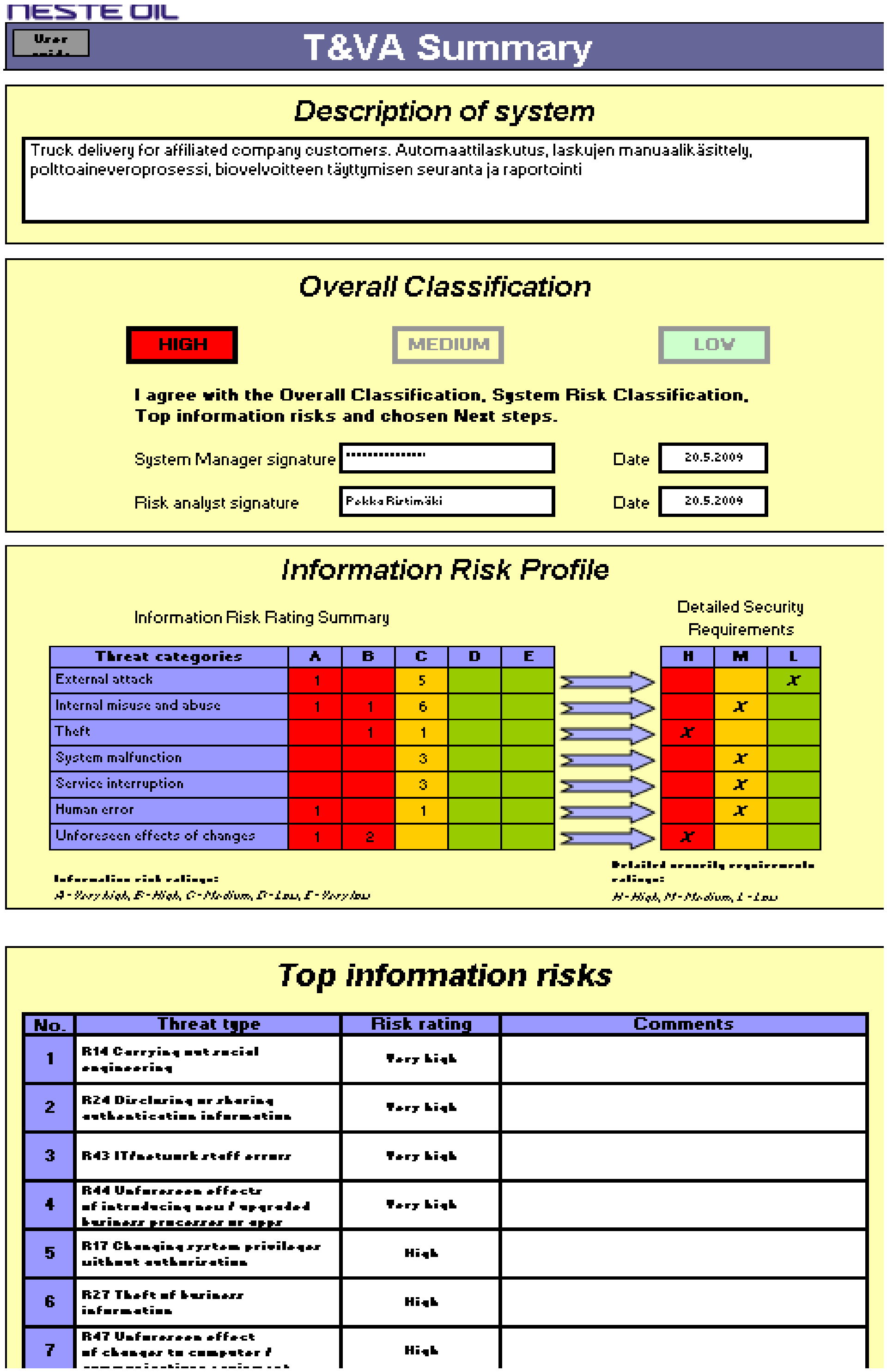
	12 hours	1 day	2-3 days	1 week	3-4 weeks
Time			X		

Business impact ratings:
A – Very high, B – High, C - Medium, D - Low, E - Very low

Top impact types

No.	Impact type	Impact ratings			Comments
		C	I	A	
1	F1 Loss of sales	Very high	Very low	Medium	
2	O1 Loss of management control (eg weakened decision-making)	Very low	Medium	Very high	
3	O5 Unforeseen impacts of changes in operations or systems	Medium	Very high		
4	C1 Delayed deliveries to customers or clients (eg failure to meet product delivery deadlines)	Very low	Very high		

11.10 Appendix 10: NORA T&VA Summary



User guide

T&VA Summary

Description of system

Truck delivery for affiliated company customers. Automaattilaskutus, laskujen manuaalikäsittely, polttoaineveroprosessi, biovelvoitteen täyttymisen seuranta ja raportointi

Overall Classification

HIGH MEDIUM LOW

I agree with the Overall Classification, System Risk Classification, Top information risks and chosen Next steps.

System Manager signature *************** Date 20.5.2009

Risk analyst signature Pekka Rirtimäki Date 20.5.2009

Information Risk Profile

Information Risk Rating Summary

Detailed Security Requirements

Threat categories	A	B	C	D	E	H	M	L
External attack	1		5					x
Internal misuse and abuse	1	1	6				x	
Theft		1	1			x		
System malfunction			3				x	
Service interruption			3				x	
Human error	1		1				x	
Unforeseen effects of changes	1	2				x		

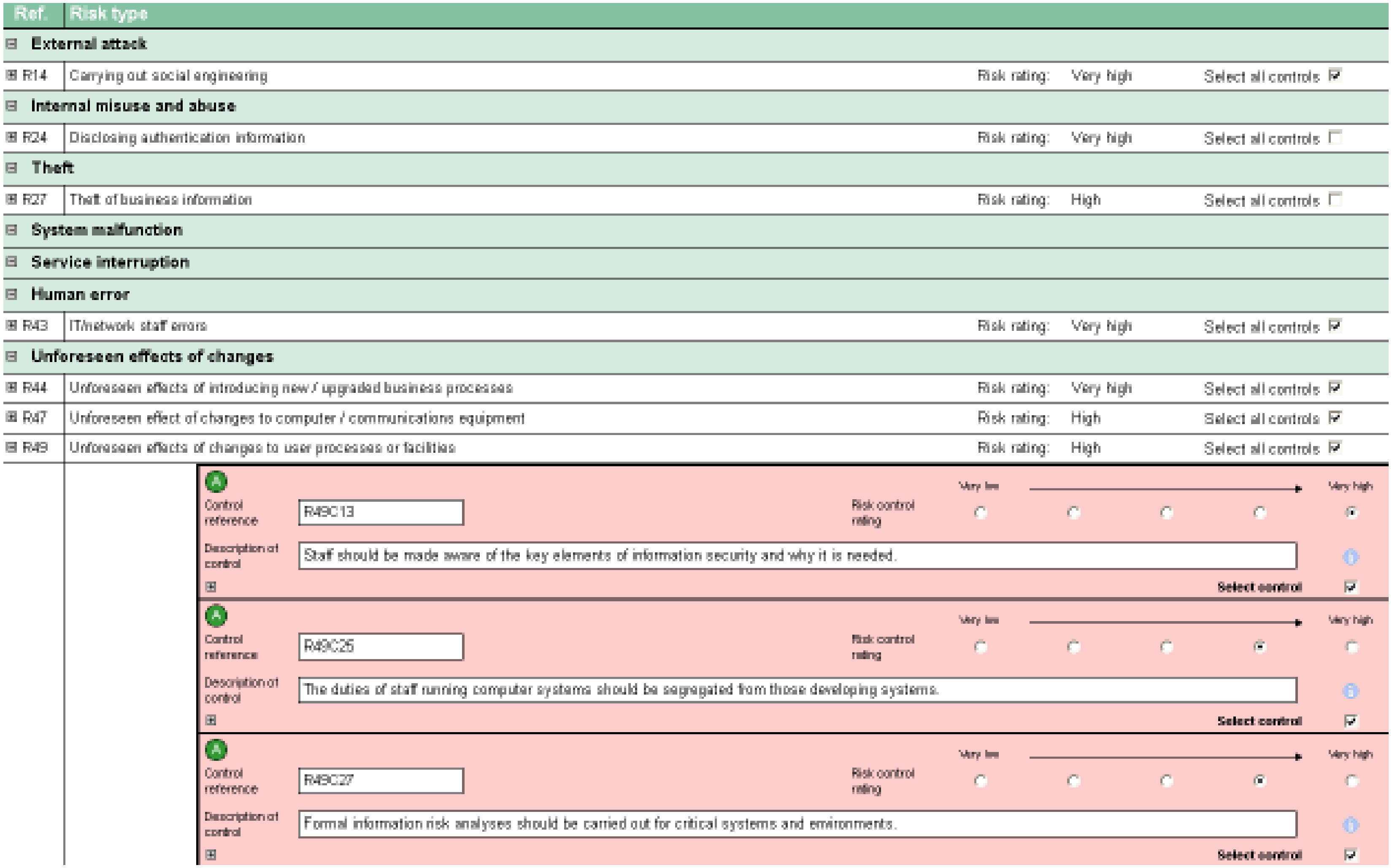
Information risk ratings:
A - Very high, B - High, C - Medium, D - Low, E - Very low

Detailed security requirements ratings:
H - High, M - Medium, L - Low

Top information risks

No.	Threat type	Risk rating	Comments
1	R14 Carrying out social engineering	Very high	
2	R24 Disclosing or sharing authentication information	Very high	
3	R43 IT/network staff errors	Very high	
4	R44 Unforeseen effects of introducing new / upgraded business processes or apps	Very high	
5	R17 Changing system privileges without authorisation	High	
6	R27 Theft of business information	High	
7	R47 Unforeseen effect of changes to computer / communications equipment	High	

11.11 Appendix 11 NORA Control Selection (CS)



Ref.	Risk type				
⊟	**External attack**				
⊞ R14	Carrying out social engineering	Risk rating:	Very high	Select all controls	☑
⊟	**Internal misuse and abuse**				
⊞ R24	Disclosing authentication information	Risk rating:	Very high	Select all controls	□
⊟	**Theft**				
⊞ R27	Theft of business information	Risk rating:	High	Select all controls	□
⊟	**System malfunction**				
⊟	**Service interruption**				
⊟	**Human error**				
⊞ R43	IT/network staff errors	Risk rating:	Very high	Select all controls	☑
⊟	**Unforeseen effects of changes**				
⊞ R44	Unforeseen effects of introducing new / upgraded business processes	Risk rating:	Very high	Select all controls	☑
⊞ R47	Unforeseen effect of changes to computer / communications equipment	Risk rating:	High	Select all controls	☑
⊞ R49	Unforeseen effects of changes to user processes or facilities	Risk rating:	High	Select all controls	☑

Control reference: R49C13

Risk control rating: Very low ○ ○ ○ ○ ● Very high

Description of control: Staff should be made aware of the key elements of information security and why it is needed.

⊞ **Select control** ☑

Control reference: R49C25

Risk control rating: Very low ○ ○ ○ ● ○ Very high

Description of control: The duties of staff running computer systems should be segregated from those developing systems.

⊞ **Select control** ☑

Control reference: R49C27

Risk control rating: Very low ○ ○ ○ ● ○ Very high

Description of control: Formal information risk analyses should be carried out for critical systems and environments.

⊞ **Select control** ☑